UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

SUSAN B. LONG, DAVID BURNHAM, and TRAC REPORTS, INC. Plaintiffs, v. U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, and U.S. CUSTOMS AND BORDER PROTECTION, Defendants.	Civil Action No.: 5:23-cv-01564 (DNH/TWD)

DECLARATION OF NATE FONTAINE

Nate Fontaine declares the following under the penalties of perjury:

1. I serve as the Chief Information Security Officer within the Office of the Chief Information Officer (OCIO) for U.S. Immigration and Customs and Immigration Enforcement (ICE) within U.S. Department of Homeland Security (DHS). I am responsible for maintaining ICE information security through a proactive and risk-based approach. In summary, the function of ICE OCIO's responsibility mission is to provide infrastructure, governance, cyberdefense and incident response capabilities, and oversight to deliver mission capabilities securely, efficiently, and effectively. As such, I make this declaration based on my personal knowledge, training, and experience as well as information provided to me by other ICE employees in the course of my official duties and my review of records kept by ICE in the ordinary course of business. I make this declaration in support of ICE's Motion for Summary Judgment in this case.

2. While ICE believes Plaintiffs do not intend to increase the risk of a cyberattack against ICE or to decrease ICE's cybersecurity through Plaintiffs' FOIA request, it nevertheless is a reality that producing records responsive to Plaintiffs' FOIA request exposes ICE to risks and dangers of cyberattacks, which could reasonably have consequences for ICE as well as the subjects of the information contained within the Enforcement Integrated Database ("EID").

PLAINTIFFS' FOIA REQUEST

3. I make this Declaration in response to the Plaintiffs' proposal submitted on August 1, 2024, which I have been told is the operative FOIA request for these purposes. In the August 1, 2024, letter, Plaintiffs request that ICE produce the following three subsets of records from the EID:

a. "All datapoints (from any time) that are directly or indirectly linked to a person for whom the Agencies have established an official case seeking that person's removal from the country." ("Part 1").

b. "All datapoints (from any time) that are directly or indirectly linked to a person who was apprehended pursuant to a Customs and Border Protection (CBP) "encounter" in or after Fiscal Year 2020, with "encounter" used to mean the same thing that CBP uses it to mean in its Nationwide Encounters Dataset." ("Part 2").

c. "All code files, lookup tables, or other records that translate the specific codes used in connection with the datapoints contained in paragraphs (1) and (2) above into their corresponding meaning." ("Part 3").

THE EID IS DESIGNATED AS A DHS HIGH VALUE ASSET AND MISSION-ESSENTIAL SYSTEM

4. By way of background, the EID is a DHS shared law enforcement database that is used daily by thousands of ICE officers, agents, and other law enforcement personnel in the execution of their duties. The EID contains data used jointly with other federal agencies and law enforcement partners, including the Federal Bureau of Investigation, U.S. Drug Enforcement Administration, U.S. Department of State, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, and the U.S. Marshals Service. The EID interfaces with many other systems and is considered a Mission Critical System. Catastrophic failure of the system, or unauthorized disclosure of law enforcement data in the system, could significantly disrupt ICE's law enforcement mission.

5. The High Value Asset (HVA) Initiative, which began in 2015, was a step to help federal agencies to recognize, categorize, and prioritize "crown jewel" systems and provide them with a sustained and sophisticated defense. In its Memorandum for Management of Federal High Value Assets (M-17-09), the Office of Management and Budget (OMB) has defined HVA as "those assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.[1]"

[1] Memorandum for Management of Federal High Value Assets (M-17-19), Archives.gov, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-09.pdf

6. The Office of Management and Budget, in Memorandum M-19-03, provided agencies with an approach to HVA identification, which allows agencies to have greater flexibility in the identification and designation of their most critical assets. An agency may designate a federal information system as an HVA when it relates to one or more of the following categories:

a. Informational Value: The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.

b. Mission Essential: The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF) as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.

c. Federal Civilian Enterprise Essential (FCEE): The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

7. The EID has been designated by ICE/DHS as an HVA, which means unauthorized disclosure or loss of control of any element of the EID could cause *exceptionally grave harm* to the United States. The EID qualifies for all three categories above (Informational Value, Mission Essential, and Federal Civilian Enterprise Essential), and supports ICE's primary, mission-essential functions, making it of specific high value to criminal, politically motivated, or state-sponsored actors for either direct exploitation or to cause loss of confidence in ICE and the United States government. HVA designation is based on scoring on three dimensions noted in the NIST Standards for Security Categorization of Federal Information and Information Systems (FIPS 199). This document develops standards for categorizing information and all federal information

systems. This document provides a common framework and understanding for expressing security across the federal government:

a. Confidentiality: The level of confidentiality of the system and records within the asset. The EID contains information related to protected status aliens, terrorists, victims, witnesses, international gang members, and immigration law violators. In fact, the EID captures and holds information designated with a High FIPS categorization—the highest sensitivity level—described as information related to investigations, law enforcement, and special operational activities to include information that inaccuracy of, loss of, or unauthorized alteration of could reasonably be expected to result in a loss of life. If an attacker can exfiltrate sensitive mission-essential information from the EID, the life and safety of law enforcement agents, victims, and witnesses (among others) would be significantly compromised and could reasonably be endangered. Because various agencies contribute data to the EID and have access to the EID, the consequences of a breach would extend past ICE. Indeed, several agencies' law enforcement and national security missions would be compromised with the disclosure of mission-essential case information in the EID.

b. Integrity: The level of data integrity that is required. It is mission-essential that data in the EID must be accurate and reliable. If a known cyberattack modifies or deletes data, the ICE mission is unachievable. If a cyberattack is not discovered, there is greater potential that data will be modified or deleted, and would paralyze ICE's mission. A cyberattack could reasonably allow bad actors to perform bad acts, cause physical harm to diverse groups of people, be released from custody, disclose law enforcement techniques and procedures, evade investigation, interfere with enforcement proceedings, and

otherwise evade law enforcement. A cyberattack also would allow bad actors to identify people (including witnesses, family members, and confidential sources, as well as government employees, among others) based on information contained in the EID, including but not limited to Social Security Numbers, home addresses and telephone numbers. This identification would constitute a clear and unwarranted invasion of privacy for those individuals.

c. Availability: The EID database, which supports various law enforcement operations within and without ICE, must be available 24 hours per day, 7 days per week, 365 days per year. If the system became unavailable or inaccessible by virtue of a cyberattack, it would cause irreparable harm to ICE missions and functions as well as its image and reputation, such that the catastrophic result would not be able to be repaired or set right again. Further, ICE would not have the ability to efficiently share immigration and detention data with other DHS and law enforcement components, including CBP Office of Field Operations, Citizenship and Immigration Services, U.S. Department of Justice (DOJ), Federal Bureau of Investigations, Department of State, and other agencies, whose missions would likewise be affected.

8. A cyberattack that renders the EID unavailable or inaccessible could also result in loss of major tangible assets or resources, including posing a threat to physical safety and/or human life. ERO, CBP, and other agencies use the information in the EID to identify previous criminal status of individuals. Not having access to this information could reasonably slow down or even result in officials misidentifying, or categorizing, the risk to public safety and risk of flight posed by a violent individual arrested for immigration violations. Additionally, agencies utilize the EID to document noncitizens that are in custody. If this information is unavailable it would impact the

care and feeding of our detained population, to include critical medical care.

THE EID SYSTEM DESIGN RECORDS ARE LAW ENFORCEMENT SENSITIVE, CYBERSECURITY SENSITIVE, AND CONTAIN CONTROLLED UNCLASSIFIED INFORMATION; DISCLOSING WOULD INCREASE CYBER-CRIMINALS' ABILITY TO HARM ICE'S MISSION AND THE SUBJECTS OF THE DATA

9. Plaintiffs seek data from the EID and further seek to control ICE's production. Specifically, Plaintiffs seek to have ICE's production preserve "relational information" (Plaintiffs' term). Plaintiffs also seek data "directly or indirectly" linked to an individual.

10. If ICE made production as requested by Plaintiffs, ICE would also expose EID system configurations, system keys for interconnected relationships, and the data within the systems, which are compiled for law enforcement purposes. This broader information about the EID constitutes law enforcement sensitive information and is also cybersecurity sensitive. It also would disclose law enforcement techniques and procedures.

11. Disclosing this information could reasonably result in increased opportunities for bad actors to attack the EID and associated systems, to gain access to personally identifiable information (PII) related to noncitizen subjects of the records, other individuals (such as witnesses to crimes or family members) whose identities are contained in the records, ICE personnel, and others involved in the immigration process. Further, disclosing this information could reasonably allow bad actors a greater opportunity to predict law enforcement actions, to commit crimes, and to evade law enforcement.

12. Our nation is experiencing an increasing volume of sophisticated cyberthreats. These threats are real. These threats continue to grow in sophistication and severity as technology advances and bad actors continue to invest in cyberattacks for their own ends.

13. Government agencies, and in particular federal law enforcement agencies, have emerged as a prime target for cybercriminals. Christina Quinn, commander of Fairfax County Police Department Cyber and Forensic Bureau and Chair of the International Association of Chiefs of Police, argued that law enforcement "across the country suffered numerous ransomware attacks in 2021 and are likely to see continued ransomware attempts."[2]

14. These threats have materialized. On a daily basis, U.S. government systems and law enforcement systems are subjected to complex and dangerous cyberattacks. Here are ten examples—out of many—of cyberattacks from the past decade, which illustrate the real risks posed by cyberattacks and the effects those attacks can have:

a. In June 2015, the U.S. Office of Personnel Management (OPM) announced two separate but related cyberattacks that impacted the personally identifiable data of Federal government employees, contractors, and others. Records stolen included Social Security numbers, background investigations records, fingerprints, and financial history for over 20 million individuals. Earlier the same year, a cyber criminal breached the OPM database and stole the full name, birth date, home address and Social Security Numbers for over four million current and former Federal government employees.[3]

---

[2] Pattison-Gordon, Julie, *Are police departments ready for cyber threats 2022 will bring?*, Govtech.com (January 20, 2022), https://www.govtech.com/security/are-police-departments-ready-for-cyber-threats-2022-will-bring.

[3] *Cybersecurity Incidents: What Happened*, https://www.opm.gov/cybersecurity/cybersecurity-incidents (last visited May 5, 2023).

b. In June 2020, a cyberattack dubbed "BlueLeaks" was conducted in which criminals stole data related to law enforcement tactics and procedures of over 200 state, local and federal agencies spanning 24 years. Criminals also stole highly sensitive data related to names, email addresses, phone numbers and banking information of individuals.

c. In 2020, a major cyberattack known as "SolarWinds" impacted 425 of the Fortune 500, the top ten telecommunications companies in the United States, the top five accounting firms in the United States, all branches of the United States Military, the Pentagon, the Department of State, the Department of Homeland Security, Department of Commerce, Department of Agriculture, Department of Treasury, Department of Energy, and the Administrative Office of the United States Courts as well as hundreds of universities and colleges worldwide. The attackers kept a minimal malware footprint, preferring to steal and use credentials to perform lateral movement through the network and establish legitimate remote access.

d. In 2021, the District of Columbia Police Department suffered a massive cyberattack in which perpetrators released thousands of sensitive documents on the dark web. The Associated Press found "hundreds of police officer disciplinary files and intelligence reports that include feeds from other agencies, including the FBI and Secret Service."[4] Other items released include documents detailing security information related to President Biden's inauguration, identities of confidential informants, and records of disciplinary proceedings that included the personally identifiable information of hundreds

[4] Alan Suderman, *DC Police Victim of Massive Data Leak by Ransomware Gang*, (May 13, 2021) https://apnews.com/article/police-technology-government-and-politics-1aedfcf42a8dc2b004ef610d0b57edb9.

of officers.

e. Later in 2021, the FBI discovered a cyberattack on its Law Enforcement Enterprise Portal platform used by U.S. law enforcement agencies and intelligence agencies to provide investigative tools and analytical resources for responding to law enforcement emergencies. This followed another 2021 cyberattack on U.S. Attorneys' offices in which employee email accounts were compromised.[5]

f. In February 2022, two hackers gained unauthorized access to the Drug Enforcement Administration database that contained detailed, non-public records related to narcotics and currency seizures and law enforcement intelligence reports. The hackers used information obtained from the DEA database to impersonate law enforcement officers to gain access to information about social media companies' users.[6]

g. In early 2023, the FBI confirmed a cyberattack against its New York Field Office that affected a computer network used in child sexual exploitation investigations. In this incident, the cyber attacker entered the system and injected a virus, according to FBI Crimes Against Children Coordinator in New York.[7]

---

[5] Sean Lyngaas, *Fake FBI Emails about a Sophisticated Attack Are Part of 'Ongoing Situation,' Agency Says,* (November 14, 2021) https://www.cnn.com/2021/11/13/politics/fbi-fake-emails-cyber-threat.

[6] U.S. Attorney's Office, Eastern District of New York, March 14, 2023, *Two Men Charged for Breaching Federal Law Enforcement Database and Posing as Police Officers to Defraud Social Media Companies*, [Press Release] https://www.justice.gov/usao-edny/pr/two-men-charged-breaching-federal-law-enforcement-database-and-posing-police-officers.

[7] Nihal Kirshan, *FBI Says Cyber Incident at New York Field Office 'Contained'*, Fedscoop (February 17, 2023) https://fedscoop.com/fbi-cyber-incident.

h. That same month, cyber attackers penetrated the Modesto California Police Department database. Effects included "downing patrol vehicles' mobile data computers for five weeks, preventing police from using them to check for individuals' criminal histories or outstanding warrants." The cyber attackers released "all kinds of sensitive information on the internet, including names of law enforcement informants, investigations into child abuse allegations, and personnel evaluations."[8]

i. And, yet again in the same month, the U.S. Marshals Service (USMS) discovered it was the victim of a major cyberattack in which hackers stole law enforcement-sensitive data related to ongoing investigations, personally identifiable information related to subjects of USMS investigations, personally identifiable information related to employees, and internal techniques and procedures. USMS was the subject of a different cyberattack about three years earlier in which personally identifiable information related to almost 400,000 current and former federal inmates, and third parties, were released.

j. The next month, both the Camden County, New Jersey Police Department and the Camden County Prosecutor's Office experienced a cyberattack that locked the agency's criminal investigative files and day-to-day internal administrative abilities. There is significant concern that, where troves of sensitive law enforcement information have been accessed, prosecutions may "be dropped due to lost or compromised evidence," based on prior incidents.[9]

---

[8] *Modesto Police Department Breach May Have Gone Days without Discovery*, The Modesto Bee (March 29, 2023) (https://insider.govtech.com/california/news/modesto-police-department-breach-may-have-gone-days-without-discovery).

[9] Jonathan Greig, *New Jersey County Police Department Confirms Ransomware Attack*, The

15. As a result of the sharp increase in sophistication and methods of cyberattack, DHS and its components, including ICE, have been required to increase security controls and methods to "keep up" with the bad actors seeking to cause harm to the individuals whose records are maintained by DHS and ICE.

16. Numerous federal policies, regulations, executive orders, and directives underscore the seriousness with which the U.S. government is striving to protect its information assets.

17. Executive policy recognizes these ever-growing threats. For example, on May 12, 2021, President Biden issued Executive Order 14028, "Improving the Nation's Cybersecurity." The Executive Order states that the United States "faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." The Executive Order provides the following directive: the "Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid." Moreover, the Executive Order codifies an executive policy priority: "the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." Likewise, Deputy Attorney General Lisa O. Monaco has stated the risk of cyber threat "has exploded" in recent years and, at the same time, "has become more diffuse, more sophisticated, more dangerous than ever before."[10] She

---

Record (April 7, 2023) https://therecord.media/camden-county-police-ransomware-new-jersey-philadelphia.

[10] Annual Munich Cybersecurity Conference (February 17, 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security.

also stated, "the criminal groups and the threats that they pose now have a national security overlay, they have clear national security implications."[11]

18. More broadly, many laws, policies, regulations, executive orders, and directives have been developed, implemented, and updated recently to accommodate the dramatic rise in the volume and sophistication of cyberattacks against federal agencies over the past decade. Here are nine examples (among others) of recent updates to policy and regulation reflecting the risks posed by attacks:

a. *The Federal Information Security Modernization Act (FISMA) of 2014* established the authority for DHS to administer the implementation of agency information security policies and practices for information systems. DHS requires federal agencies, including ICE, to provide information security to address evolving risks to the information and systems that support the operations and assets of the agency. It requires federal agencies to implement security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, modification, or destruction of (1) information collected/maintained by or for the agency; and (2) information systems used or operated by an agency or by a contractor of an agency.

b. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), outlined actions that agencies must now take to enhance cybersecurity and reinforced FISMA 2014. It states in part that agency heads "will be held accountable by the President for implementing risk management

[11] Criminal Division Cybersecurity Roundtable: The Evolving Cyber Threat Landscape (Oct. 20, 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr.

measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data." Executive Order 13800 further required agencies to follow The Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"), developed by the National Institute of Standards and Technology, to manage cybersecurity risk and provide justification for actions taken to mitigate or accept cybersecurity risk.

c. Executive Order 14028, Improving the Nation's Cybersecurity (May 21, 2021), addressed the marked increase in cyberattacks against the Federal Government—and directed "bold changes and significant investments" and that the scope of protection and security must include "systems that process data (information technology) and those that run the vital machinery that ensures our safety (operational technology). It states in Section 1, "It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security." It additionally directed each agency to implement a "Zero Trust Architecture" approach to cybersecurity.

d. "Zero Trust Architecture" (ZTA) "means a security model, a set of system design principles, and a coordinated cybersecurity and management strategy based on acknowledgement that threats exist both inside and outside traditional network boundaries. Zero Trust Architecture allows users full access but only to the *bare minimum* they need to perform their jobs. This means using ultra-specific risk-based access controls--known as "least-privilege" access to data or information technology resources. The answers to who, what, when, where and how are critical for appropriately allowing or denying access…." (Executive Order 14082, at Sec. 10(K)). ZTA requires that very few ICE personnel could

be authorized to access or read the EID system design records that Plaintiffs seek to be released publicly.

e. DHS issued Policy Directive 4300A, Information Technology System Security Program, Sensitive Systems (September 20, 2022), which established the current information security policy for DHS to accommodate the latest threats to the agency's systems and data.

f. Office of Management and Budget (OMB) Memorandum M-17-09, Management of Federal High Value Assets, addresses the agency's obligations related to High Value Assets such as the EID. It addresses the steps to be taken to protect the Federal Government's critical networks, systems and data for which unauthorized access, use, disclosure, disruption, modification or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to public confidence, civil liberties, or public health and safety of the American people.

g. OMB Circular A-130, Managing Information as a Strategic Resource, requires agencies to manage Federal information throughout the information lifecycle and directs agencies to provide protection for their information commensurate with the current risk level and potential harm resulting from its compromise.

h. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, provides guidelines for applying the Risk Management Framework to federal information systems, to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control

monitoring. This allows the agency to document its unique situation and methods used to combat cyber-threats.

i. Federal Information Processing Standard (CFIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, directs agencies to categorize their information and information systems based on the potential impact to an organization should events occur which jeopardize the information and information systems of an organization. It lays out the criteria for categorization of systems according to risk and tailoring security according to risk assessment. This means agencies will list their highest-priority systems and direct resources as needed to protect and monitor those highest value systems to the maximum extent.

A CYBERATTACK ON THE EID COULD CAUSE LONG-TERM DATA LOSS AND DAMAGE TO LAW ENFORCEMENT SYSTEMS, TO LAW ENFORCEMENT MISSIONS, TO NATIONAL SECURITY, TO PUBLIC SAFETY, AND TO THE TRUST, LIFE AND SAFETY OF SUBJECTS, CONFIDENTIAL INFORMANTS, WITNESSES, ICE EMPLOYEES, AND OTHER PROTECTED INDIVIDUALS

19. Cyberattacks have consequences that reach beyond the immediate effects of the attack, explained above, which include preventing law enforcement missions as well as compromising data and systems. Cyberattacks would also have long-term consequences that could reasonably heavily impact ICE's capacity to fulfill its congressionally mandated law-enforcement mission now and far into the future. But the consequences of a cyberattack would also negatively impact the mission of all federal and law enforcement agencies with whom ICE shares data through the EID.

20. First, there are tangible short-term effects associated with a cyberattack on the EID. A cyberattack on the EID could lock the database (as in a ransomware attack or in an attack by an actor seeking to foil ICE's investigations), and all the data within the database, or otherwise make it inaccessible, which would impact ICE's ability to identify, arrest and detain individuals who are terrorists, national security threats, threats to public safety, and otherwise in the United States illegally. Officers would be unable to use the database to determine an encountered individual's criminal history, fingerprints and other biometrics, and other factors essential to understanding the threat that individual may represent to the public. This could reasonably result in ICE officers being required to release dangerous individuals who would otherwise be arrested—thus impacting national security and public safety.

21. Second, there are several long-term effects that a cyberattack could reasonably have on ICE and its law-enforcement partners. One long-term and significant consequence of an attack on the EID is that the mere one-time presence of an attacker in a law enforcement database, known as a "broken chain of custody" of sensitive law enforcement data, can compromise the integrity and reliability of the database and all the data contained within—potentially forever. Bad actors often lock down data, modify data, or delete data, which could render evidence and case information contained in the EID inadmissible in court. If data remained inadmissible, ICE's ability to conduct its law enforcement mission, and data related to millions of individuals contained in the EID, could become almost nonexistent in a worst-case scenario. ICE could be placed in a position where it cannot present reliable or valid data to support enforcement actions. Thus, it is possible that individuals who present a threat to national security or public safety would be released due to lack of usable data related to those enforcement actions.

22. Another long-term effect of an attack on the EID is that cyber attackers often release illegally retrieved records to the public, which would constitute a clearly unwarranted invasion of personal privacy of the individuals involved and which could reasonably constitute an unwarranted invasion of the personal privacy of third parties. If a third party released EID data related to law enforcement techniques and procedures to the public, ICE would suffer significant mission impact. The public's awareness of sensitive law enforcement techniques and procedures would allow the reasonably foreseeable harm that the information would be used to commit illegal acts and evade law enforcement. It would allow bad actors to predict enforcement actions and not only to personally evade law enforcement, but to organize a group effort to break the law and evade law enforcement.

23. Attackers are also known to publicly release records containing personally identifiable information (PII) data. The EID contains sensitive PII of the subjects of the records, witnesses to crimes, sources, participants in the immigration process, and ICE officers and other law enforcement personnel.

24. Information regarding law enforcement personnel would include their full names, badge numbers, work assignment locations and hours, and numerous other sensitive data points related to law enforcement personnel. A cyberattack that resulted in public release of these data points would allow a bad actor to harass or threaten the safety of ICE and ICE contractor personnel due to the reasonably foreseeable opportunity to predict the location and techniques of officers. Bad actors could also cross-check officer PII with other publicly available data sources for the purpose of heightening their ability to threaten, harm or kill ICE employees and contractors.

25. Attackers might also publicly release sensitive noncitizen PII records, such as name, date of birth, address, country of origin, full criminal records, biometric identifiers, unique identifiers, asylum status, and immigration enforcement records. A release of sensitive PII related to noncitizens—including witnesses, informants, asylum seekers, crime victims, and other protected individuals—could significantly increase risk to those individuals. Bad actors seeking to harm particular people could use that information to locate, threaten, intimidate, harass, harm, or kill those vulnerable individuals.

DISCLOSING HOW THE EID CHANGES OVER TIME REVEALS LAW ENFORCEMENT TECHNIQUES AND PROCEDURES AND CONSTITUTES A CYBERSECURITY THREAT TO THE EID, WHICH IS A DHS HIGH VALUE ASSET

26. In the past, ICE inadvertently disclosed certain EID information pertaining to prior versions of Part 3 of the current FOIA request. Over time, Plaintiffs have obtained, compiled, and publicly released information related to the existence of EID field names. This information was obtained through FOIA requests seeking specific fields, by exact field name. ICE responded by providing records or replying that such a field did not exist. The ICE responses to the FOIA requests resulted in the confirmation that certain fields did, or did not, exist.

27. In a prior litigation, Plaintiffs were provided additional versions of the data dictionaries for the EID, along with "Code Lookups" for each. In prior litigation, ICE disclosed former versions of the EID data dictionaries, and even discretionarily created "Code Lookups" documents parallel to those versions of the data dictionaries, for the sake of resolution of the case and as a gesture of good will. The disclosed "Code Lookups" records did not exist as a record and had to be created manually by senior database experts by analyzing each table and field in the database, pulling each code for each table, and compiling them in one excel document.

28. Gathering numerous versions of the data dictionaries and other database records, in itself, reveals the latest and least publicly known law enforcement techniques. Over time, as law enforcement techniques and procedures evolve, databases containing the information gained by these techniques (including the EID) must evolve alongside those changes to allow the data to be kept and maintained. For example, if ICE developed a new law enforcement technique or procedure related to arrests, the EID data dictionary, and other EID data, would be modified to allow entry of a new or modified field for arrest data to reflect the new technique or procedure. If the updated version of the data dictionary with relational keys and system interconnections was then disclosed, and compared to prior versions, the public would become aware of the differences between data dictionary versions, as well as the latest change in law enforcement techniques and procedures. Thus, the latest and least publicly known techniques and procedures would be revealed, which would allow bad actors to anticipate law enforcement actions, to commit crimes, and to evade law enforcement.

COMPLYING WITH PLAINTIFFS' FOIA REQUEST WOULD REQUIRE REDACTING SEVERAL FIELDS AND THE INTERRELATIONSHIP BETWEEN THE FIELDS TO PROTECT FROM CYBERSECURITY AND OTHER RISKS PRESENTED BY PLAINTIFFS' REQUEST

29. Even if ICE were ordered to comply with Plaintiffs' FOIA request, there would still be the issue of fields that would need to be redacted because of FOIA exemptions.

30. Disclosing of certain details of the EID data structure (which Plaintiffs seek to have ICE preserve in production), such as foreign keys, primary keys, references to other databases or system names, references to the offices organizational structure, and data type descriptions, would expose critical and high value law enforcement systems to significant cybersecurity risks.

31. Previously, a judge sitting in the United States District Court for the District of Columbia analogized releasing the EID data structure as presenting cybersecurity risks akin to providing a thief with a map of an art museum. If that thief's map is a current version, which shows or lists where each item currently exists and which exits are currently under surveillance, that map holds greater potential to assist the thief in perpetrating a heist. The map would also show connecting tunnels with other museums significantly reducing research to move laterally through the connected museums.

32. The risks of disclosure here presents cyber risks that include, but are not limited to, an increased likelihood of targeted cyberattacks, increased potential for successful data breaches, and unauthorized access to sensitive information. Cyber breaches are rarely caused by a single point of failure. Indeed, cyber breaches are typically caused by a combination of vulnerabilities, which can include misconfigurations, weak access controls, poor data validation, and human error for example. All of these single issues align to create a pathway for attackers. Major breaches occur in organizations that believed they were well-defended, with robust security measures in place. Unidentified and underestimated weaknesses across various layers of their systems compound over time. These cumulative points of weakness are diffuse and, to uncover them usually requires synthesizing disparate information. However, producing a large quantity of data—with interconnections between the data preserved—would provide a consolidated, macro-level view of these potential weaknesses in one source. This type of disclosure makes a cyber attacker's job easier and would present unique and severe cybersecurity threats alongside a master key to the database fields. This type of disclosure could also provide a trove of information regarding various potential weak points to potential cyber attackers.

33. Additionally, Plaintiffs' FOIA request would reveal the EID database structure, which would raise two cybersecurity issues. First, disclosing the linkage between tables—which Plaintiffs seek insofar as they seek to preserve what they term as "linkage fields" or "relational information" in their request—would provide potential attackers with vital information on how the database is structured. The EID links data through primary keys and foreign keys. Primary Keys are unique identifiers for records within a table, typically a unique ID or code for each entry. One way to think about a primary key is that it establishes a *single address* where data resides within the database, from which the data can be linked to other places within the database. Foreign Keys are used to establish relationships between tables in a database, which allows data to appear in another table.

34. Cybersecurity threat actors conduct extensive research on their targets using publicly available information before launching their attacks. Through open-source intelligence, attackers can gather insights into websites, databases, and past disclosures identifying weak spots in infrastructure, personnel or security practices. This reconnaissance allows them to craft tailored attacks that exploit an organization's weaknesses.

35. From a cybersecurity perspective, attackers can use the knowledge of "relational information" (i.e. primary keys and/or foreign keys) to craft highly targeted injection attacks, which are among the most prevalent attacks used against databases in two ways:

a. **Injection Risks**: When attackers know the relationships between tables via Foreign and Primary Keys, they can inject malicious queries that traverse the database, leading to data exfiltration or even deletion of sensitive data. Injection attacks allow malicious actors to manipulate a query to gain unauthorized access or alter the database. This type of risk has materialized before. For example, security researchers found SQL

injection vulnerabilities that allowed unauthorized individuals to potentially bypass airport security screenings. A third-party application used by airlines to manage the Known Crewmember and Cockpit Access Security System allows authorized aircrews to bypass TSA airport security screening. The vulnerability allowed malicious code to be entered and authenticate the researchers as a system administrator. The researchers were able to add fictitious employees and grant them access to the TSA initiative above. The fictitious employees could then bypass security checkpoints and have access to aircraft and airport facilities not intended for public access.[12]

b. **Enumeration of Relationships**: Knowing the structure of data relationships enables attackers to map out the organizations data storage. They can infer sensitive data patterns (e.g. user accounts linked to sensitive records), allowing them to conduct account enumeration or escalate privileges, meaning, the attacker is actively gathering information about available user accounts on a system and using that information to gain access to higher levels of permission on a system. Per OWASP (Open Web Application Security Project), database relationships can also be leveraged to exploit cascading deletions or updates, leading to widespread data corruption.[13]

---

[12] BleepingComputer.com "Researchers find SQL injection to bypass airport TSA security checks". https://bleepingcomputer.com/news/security/researchers-find-sql-injection-to-bypass-airport-tsa-security-checks/.

[13] OWASP (Open Web Application Security Project). "SQL Injection" OWASP Community Documentation https://owasp.org/www-community/attacks/SQL_Injection.

36. Second, references to other databases or systems reveal crucial information about the organization's information technology infrastructure. Malicious actors can leverage this information to perform network mapping, which is the process of discovering devices, systems, and interconnections in a network. Again, there are two categories of risk to consider:

a. **Network Mapping and Reconnaissance**: Attackers who know the names and relationships of internal systems can target specific databases for attack. This process is often a precursor to lateral movement, where attackers compromise one system and then move to others within the same network to access sensitive data. This is particularly dangerous in environments where multiple systems share data (such as the EID).

b. **Exploitation of Inter-Database Relationships**: If attackers know how different systems are connected, they may exploit vulnerabilities in one system or attack another. For example, vulnerabilities in a system could be used as an entry point to access other systems by navigating through system inter-connections.[14] These risks have materialized in the past. For example, in 2013, a Target Store breach was partially enabled by attackers gaining entry into the network through a third-party HVAC vendor, then moving laterally to the payment processing system. The breach resulted in the exfiltration of personal and financial information for 110 million customers.[15] Exposing inter-database references would provide attackers with a roadmap for similar movements within a network.

---

[14] Verizon Data Breach Investigation Report (DBIR), 2022. "Understanding the Pathway of Lateral Movement in Data Breaches".

[15] CNN Business, 2014. "HVAC vendor eyed as entry point for Target breach". https://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html.

37. A separate and distinct category of risk involves revealing the organization's internal structure, including how departments interact with the data, which poses a serious risk of social engineering and spear-phishing attacks. Attackers can use this knowledge to craft highly targeted emails or communications aimed at tricking employees into giving up sensitive information or credentials. In short, revealing the internal structure of an organization can allow attackers to craft a message that appears legitimate (e.g. impersonating IT staff requesting access to the database, or impersonating law enforcement partners with information from information releases to get additional sensitive information or access) but is aimed at undermining security. For example, networking firm Ubiquity Networks disclosed in 2015 that cyber threat actors stole $46.7 million through a successful spear-phishing campaign. The cyber threat actors impersonated other executive personnel and made fraudulent requests from an outside entity to their finance department.[16] The release of internal database structure and related organizational details would make it easier for cyber threat actors to target specific employees within our organization with similar tactics.

38. Finally, even providing data type descriptions can provide detailed information how data is stored and what data types the system supports. This can allow attackers to better understand the database's vulnerabilities in two ways:

a. **Attack Surface Discovery**: If attackers know certain fields only accepts numeric data or that certain data types have strict input validation rules, they can either avoid attacking those fields or focus on less protected areas. Conversely, other fields with less validation (accept a wide range of inputs) can be exploited for injection attacks.

---

[16] KrebsonSecurity. "Tech Firm Ubiquiti Suffers $46M Cyberheist". Tech Firm Ubiquiti Suffers $46M Cyberheist – Krebs on Security.

b. **Format Specific Exploits**: Format specific exploits and deserialization attacks have emerged as critical vulnerabilities, particularly where data type descriptions and handling mechanisms are disclosed. If certain data types (e.g. serialized objects or binary fields) are disclosed, attackers might exploit known vulnerabilities in the handling of those data types such as deserialization attacks. In deserialized attacks the attacker sends a malicious crafted serialized object (remote code execution and privilege escalation) to the application, which can allow the attacker to execute code within the application. Remote code execution can allow cyber threat actors to open backdoors, steal sensitive data, and alter system configurations.

39. For example, one of the largest credit card data breaches in history involved exploits in poor input validation of Heartland Bank in 2008. Heartland's systems processed financial data, including credit card numbers but failed to validate and sanitize inputs properly. The attackers were able to inject commands into forms and fields expecting numerical values, enabling them to access over 130 million records of sensitive financial information.[17] Data type descriptions would assist attackers in identifying similar vulnerabilities in an organization's systems.

40. For these reasons, Plaintiffs' FOIA Request, if complied with, would expose ICE and the EID to increased cybersecurity risks and would reveal information protected from disclosure under FOIA.

---

[17] KrebsonSecurity. 2013. "Hacker Ring Stole 160 Million Credit Cards". https://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/

CONCLUSION

41. In conclusion, withholding details such as Foreign Keys, Primary Keys, references to other systems, organizational structures, and data type descriptions from public release is essential to protect the integrity of an organization's systems. The release of such information could provide attackers with a roadmap to exploit vulnerabilities, launch targeted attacks, and compromise sensitive systems availability and integrity. For these reasons, the decision to withhold these elements is critical for safeguarding our network, mission, and law enforcement essential data.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge and belief. Signed this 1st day of October, 2024.

NATHANIEL O FONTAINE

Digitally signed by NATHANIEL O FONTAINE
Date: 2024.10.01 10:54:20 -04'00'

NATE FONTAINE